Akin Gump
STRAUSS HAUER & FELD LLP

MICHELLE A. REED
+1 214.969.2713/fax: +1 214.969.4343
mreed@akingump.com

December 28, 2018

VIA EMAIL

New Hampshire Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Supplemental Notice Regarding Data Security Breach at OXO

To the New Hampshire Attorney General's Office:

We are contacting you again on behalf of our client, OXO International, Ltd. ("OXO"). This letter supplements the notice that was submitted to your office on October 31, 2018. Following our notice to you, OXO expanded the scope of its forensic investigation. Out of an abundance of caution and desire to protect our customers' information, OXO expanded the timeframe of potentially affected consumers. OXO is accordingly providing notice to 58 additional New Hampshire residents. Please note that in submitting this supplemental notice, OXO does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Additional Investigation

Following our original notice to you, OXO obtained additional evidence regarding the potential compromise. OXO's third-party forensic investigators conducted additional analyses and determined that the Magecart threat actor injected unauthorized, malicious JavaScript code that may have compromised customer's payment card information for a broader time period. The potentially exposed information in this incident included customer name, credit or debit card information, billing address, and shipping address. The forensic investors concluded that the malicious script contained multiple flaws that, combined with OXO site mitigations, likely limited the number of affected users. At present, the periods of potential vulnerability appear to be as follows: June 9, 2017 – November 28, 2017, June 8, 2018 – June 9, 2018, July 20, 2018 – October 16, 2018.

.

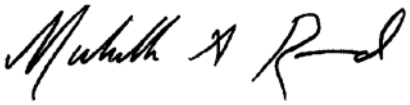
Steps to Protect Your State Residents

OXO is providing all potentially affected residents not previously notified with written notice of the incident on or about December 28, 2018, along with our supplemental notice to you. A copy of that notice is attached, excluding any identifying information. OXO is also providing access to free identity theft protection, credit monitoring, identity theft consultation and restoration for one year for all affected individuals and information on how to protect against identity theft and fraud.

In addition to the security protections referenced in our prior notification, OXO is also in the process of implementing a monitoring system which alerts on any change made to code within its website, as well as a content security policy to prevent the customers' browsers to contact any URL not whitelisted by OXO as part of the visit to OXO's website. OXO has also retained third-party experts to conduct penetration testing on its website.

If you have any further questions regarding this incident, please do not hesitate to contact me either by telephone at (214) 969-2713, or by email at mreed@akingump.com.

Sincerely,



Michelle A. Reed

Enclosure

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to tell you about an unfortunate data security incident involving sophisticated criminal activity that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

On December 17, 2018, OXO confirmed through our forensic investigators that the security of certain personal information that you entered into our e-commerce website (https://www.oxo.com) may have been compromised. We currently believe that information entered in the customer order form between June 9, 2017 – November 28, 2017, June 8, 2018 – June 9, 2018, July 20, 2018 – October 16, 2018 may have been compromised. While we believe the attempt to compromise your payment information may have been ineffective, we are notifying you out of an abundance of caution.

What information was involved?

OXO believes that unauthorized code may have allowed access to your name, billing and shipping address, and credit card information.

What we are doing.

OXO values your business and deeply regrets that this incident occurred. Upon discovering the unauthorized code, OXO immediately took actions to secure its site by working with recognized security consultants to conduct a thorough investigation of the incident and to determine additional measures designed to help prevent incidents of this kind in the future. When OXO obtained additional evidence, it retained forensic investigators to identify past website vulnerabilities. OXO has investigated the nature of the malicious code, removed the unauthorized code, conducted systems scans and reissued access credentials. OXO has also retained outside consultants to conduct penetration testing on its website.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.
*You have until **March 28, 2019** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-877-730-4607. Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-877-730-4607, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Tessa Judge
General Counsel

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.